

Patent claims

1.-10. (canceled)

11. (new) A method for setting limit values of an access control for limiting traffic transmission in a communication network, wherein the communication network comprises a plurality of pairs of marginal nodes between which the transmission occurs, and the limit values of the access control are limit values regarding the pairs, the method comprising the following steps:

setting the limit values such that probabilities for each of the pairs related to not approving the transmission between the marginal nodes of the pair are substantially the same, and such that an overload situation in the communication network does not occur;

increasing the limit values to a minimum value at which an overload situation starts to occur, such that the probabilities are substantially the same; and

updating the limit value regarding at least one of the pairs of marginal nodes, between which a transmission occurs causing the overload situation, by setting the limit value to the minimum value.

12. (new) The method in accordance with claim 11, wherein the probabilities related to not approving the transmission between the marginal nodes of the pairs are blocking probabilities related to blocking the transmission between the marginal nodes of the pairs.

13. (new) The method in accordance with claim 11, wherein the marginal nodes include nodes of the network representing

sources or sinks of traffic of the network.

14. (new) The method in accordance with claim 11, wherein the marginal nodes are specified by ingress nodes and egress nodes of the network.

15. (new) The method in accordance with claim 14, wherein the plurality of the pairs comprises all pairs of the network consisting of an ingress node and an egress node in each case.

16. (new) The method in accordance with claim 11, wherein the overload situation is produced when in a scenario of high traffic load, in which the limit values for the access controls are still adhered to, a threshold value is exceeded on a link for the traffic transmitted over the link.

17. (new) The method according to claim 16, wherein the threshold value for the traffic transmitted over the link is assigned to the link such that in case of failure of the link, the traffic allowed within the framework of the access controls does not represent any overload.

18. (new) The method in accordance with claim 11, further comprising:

 further increasing the limit values regarding further pairs of the pairs, which for the limit value is not determined yet, in excess of the minimum value to a further minimum value at which a further overload situation starts to occur, such that the probabilities are substantially the same;
 and

 updating the limit value regarding at least one of the further pairs of marginal nodes, between which a transmission occurs causing the further overload situation, by setting the

limit value to the further minimum value.

19. (new) The method in accordance with claim 18, comprising repeating the further steps until the limit values for all of the pairs are determined.

20. (new) The method in accordance with claim 18, wherein the further overload situation is produced when in a further scenario of high traffic load, in which the limit values for the access controls are still adhered to, a further threshold value is exceeded on a further link for the further traffic transmitted over the further link.

21. (new) The method according to claim 20, wherein the further threshold value for the further traffic transmitted over the further link is assigned to the further link such that in case of failure of the further link, the further traffic allowed within the framework of the access controls does not represent any overload.

22. (new) The method in accordance with claim 11, further comprising:

making access checks for all the traffic of a class of service.

23. (new) The method in accordance with claim 22, wherein the access checks relate to an approval or rejection of individual flows.

24. (new) A network node with means for executing the method in accordance with claims 11.

25. (new) The network node according claim 24, wherein the

network node is a marginal node of the network.